CLAIMS

1. A computer-implemented method for protecting computer code from malicious retrievers, said method comprising the steps of:

generating retrieval information characteristic of data sent to a retriever by the computer code in response to a retrieval command issued by the retriever;

accessing at least one rule using at least some of said retrieval information as an input to said at least one rule; and

when said at least one rule informs that the retrieval is not acceptable, flagging the retrieval command as suspicious.

2. The method of claim 1 wherein the retrieval information comprises a retrieval vector.

3. The method of claim 2 wherein the retrieval vector comprises at least one of the following:

number of rows in the retrieval;

number of columns in the retrieval;

number of tables in the retrieval;

identification of columns in the retrieval;

identification of tables in the retrieval.

4. The method of claim 1 wherein the retrieval information comprises statistical information.

5. The method of claim 4 wherein at least some of the statistical information is contained in a state table.

6. The method of claim 4 wherein a plurality of retrieval commands are issued, and the statistical information comprises at least one of the following:

rate of retrieving rows from the computer code;

rate of retrieving columns from the computer code;

rate of retrieving tables from the computer code;

average number of rows retrieved per retrieval command for a given input vector, where an input vector contains parameterized information characteristic of the retrieval command;

average number of columns retrieved per retrieval command for a given input vector;

average number of tables retrieved per retrieval command for a given input vector;

percentage of retrieval commands for which a given column is accessed;

percentage of retrieval commands for which a given table is accessed;

percentage of retrieval commands for which a given combination of columns is accessed;

percentage of retrieval commands for which a given combination of tables is accessed.

7. The method of claim 1 wherein said at least one rule is also accessed by an input vector containing parameterized information characteristic of the retrieval command.

8. The method of claim 7 wherein the input vector is extracted from a retrieval command by at least one technique from the group of techniques comprising real-time auditing and in-line interception.

9. The method of claim 7 wherein said at least one rule is accessed by at least two input vectors, each input vector being associated with the same retrieval command.

10. The method of claim 7 wherein the input vector comprises at least one parameter from the group of parameters comprising:

canonicalized commands;

dates and times at which commands access the computer code;

logins of users that issue commands;

identities of users that issue commands;

departments of users that issue commands;

applications that issue commands;

IP addresses of issuing users;

identities of users accessing a given field within the computer code;

times of day that a given user accesses a given field within the computer code;

fields accessed by commands;

combinations of fields accessed by commands;

tables within the computer code accessed by commands;

combinations of tables within the computer code accessed by commands.

11. The method of claim 10 wherein a canonicalized command is a retrieval command stripped of literal field data.

12. The method of claim 1 wherein, when a retrieval command is flagged as suspicious, at least one of the following is performed:

an alert is sent to a system administrator;

an audit log is updated;

the command is not allowed to access the computer code;

the command is allowed to access the computer code, but the access is limited;

the command is augmented;

a sender of the command is investigated.

13. The method of claim 1 wherein the computer code is a database.

14. The method of claim 13 wherein the retrieval command is a SQL command.

15. The method of claim 1 wherein said at least one rule contains content developed during a training phase.

16. The method of claim 15 wherein said at least one rule comprises at least one rule derived from statistical information accumulated during the training phase.

17. The method of claim 15 wherein the training phase is performed in real time.

18. The method of claim 15 wherein the training phase comprises the steps of:

observing retrieval commands that access the computer code;

observing responses to the retrieval commands generated by the computer code; and

deriving from said responses a set of retrieval information.

19. The method of claim 18 wherein the step of observing retrieval commands comprises at least one of:

real-time auditing; and

in-line interception.

20. The method of claim 19 wherein the step of observing retrieval commands comprises real-time auditing; and at least one of the following is used to extract the commands for observation:

an API that accesses the computer code;

code injection;

patching;

direct database integration;

log file examination.

21. The method of claim 19 wherein the step of observing retrieval commands comprises in-line interception; and at least one of the following is interposed between senders of the commands and the computer code:

a proxy;

a firewall;

a sniffer.

22. The method of claim 18 wherein the step of observing responses to the retrieval commands comprises at least one of:

real-time auditing; and

in-line interception.

23. The method of claim 22 wherein the step of observing responses to the retrieval commands comprises real-time auditing; and at least one of the following is used to extract the commands for observation:

an API that accesses the computer code;

code injection;

patching;

direct database integration;

log file examination.

24. The method of claim 22 wherein the step of observing responses to the retrieval commands comprises in-line

interception; and at least one of the following is interposed between senders of the commands and the computer code:

a proxy;

a firewall;

a sniffer.

25. The method of claim 15 wherein a duration of performing the training phase is determined by statistical means.

26. The method of claim 15 wherein:

during the training phase, suspicious activity is tracked; and

the suspicious activity is subsequently reported to a system administrator.

27. The method of claim 1 wherein the generating step comprises at least one of:

real-time auditing; and

in-line interception.

28. The method of claim 1 wherein said at least one rule comprises at least one rule provided by a system administrator.

29. The method of claim 1 wherein said at least one rule comprises at least one rule provided by a vendor.

30. The method of claim 1 wherein said at least one rule comprises a pre-established rule table pertaining to retrievals.

31. A computer-readable medium containing computer program instructions for protecting computer code from malicious

retrievers, said computer program instructions performing the steps of:

generating retrieval information characteristic of data sent to a retriever by the computer code in response to a retrieval command issued by the retriever;

accessing at least one rule using at least some of said retrieval information as an input to said at least one rule; and

when said at least one rule informs that the retrieval is not acceptable, flagging the retrieval command as suspicious.

32. Apparatus for protecting computer code from malicious retrievers, said apparatus comprising:

means for generating retrieval information characteristic of data sent to a retriever by the computer code in response to a retrieval command issued by the retriever;

coupled to the generating means, at least one rule pertaining to retrievals; and

means for accessing said at least one rule using retrieval information as an input to said at least one rule.